WHAT IS CLAIMED IS:

1. A link lock system for a network, comprising:

a computer;

a network interface device to provide the computer with access to the network;

a bus monitor to monitor a first link between the network interface device and the computer, where said bus monitor reports detected failures or intrusions; and

a security switch to switch the first link from a non-secured mode to a secured mode when a report of said detected failures or intrusions is received from the bus monitor.

2. The system of claim 1, wherein said computer is a server.

3. The system of claim 1, wherein the network operates in a secured mode using an HTTP-S protocol.

4. The system of claim 1, wherein said non-secured mode of the first link between the network device and the computer uses HTTP protocol.

5. The system of claim 4, wherein said secured mode of the first link between the network device and the computer uses HTTP-S protocol.

6. The system of claim 1, further comprising:

a controller that receives the report from the bus monitor and sends control signals to the network interface device, the security switch, and the computer.

7. The system of claim 6, further comprising:

an encryption element in the computer, where said encryption element converts data placed on said first link to a secured protocol when the control signal is received from said controller.

8. A system for a server, comprising:

an interface device to provide the server with access to a network; and

a controller to monitor a link between the interface device and the server, where said controller switches the link from a non-secured protocol to a secured protocol when failures or intrusions are detected on the link.

9. The system of claim 8, wherein the network is Internet, such that the non-secured protocol includes HTTP and the secured protocol includes HTTP-S.

10. The system of claim 8, wherein said controller sends a control signal to the server when failures or intrusions are detected on the link.

11. The system of claim 10, further comprising:

an encryption element in the server, where said encryption element converts data placed on said link by the server to a secured protocol when the control signal is received from said controller.

12. A method, comprising:

monitoring a link between a network device and a computer;

first directing the link to use a secured protocol when failures or intrusions are detected on the link; and

second directing the link to revert to a non-secured protocol when said detected failures or intrusions have been corrected.

13. The method of claim 12, wherein said non-secured protocol includes HTTP protocol.

14. The method of claim 12, wherein said secured protocol includes HTTP-S protocol.

15. The method of claim 12, wherein the computer is a server.

16. An apparatus comprising a machine-readable storage medium having executable instructions that enable the machine to:

monitor a link between a network device and a server;

first directing the link to use a secured protocol when failures or intrusions are detected on the link; and

second directing the link to revert to a non-secured protocol when said detected failures or intrusions have been corrected.

17. The apparatus of claim 16, wherein said non-secured protocol includes HTTP protocol.

18. The apparatus of claim 16, wherein said secured protocol includes HTTP-S protocol.